WHAT IS CLAIMED IS:

1. A mutual authentication method which authenticates a mutual relationship between a first authentication device and a second authentication device being connected via a communication line, comprising,

a step for storing as history data commonly in each of said first authentication device and said second authentication device, an update result obtained by updating stored data for specifying said first authentication device and stored data for specifying said second authentication device, by use of the stored data obtained from previous authentication per authentication carried out mutually in advance between said first authentication device and said second authentication device, wherein,

said first authentication device includes,

a first transmitting step which newly generates stored data by use of the history data being stored, encrypts the thus generated new stored data by use of said history data, and transmits the encryption data to the second authentication device, and

a first updating step which updates said history data with the stored data from said second authentication device and the new stored data thus transmitted, and

the second authentication device includes,

a second transmitting step which newly generates stored data by use of the stored data from said first authentication device and the history data being stored, encrypts the thus

generated new stored data by use of said history data, and transmits the encryption data to the first authentication device, and

a second updating step which updates said history data by the stored data from said first authentication device and said new stored data thus transmitted, and

in at least one of said first authentication device and said second authentication device, when validity of the stored data is established based on the history data, it is verified that the mutual relationship between the first authentication device and the second authentication device is valid.

2. The mutual authentication method according to claim 1, wherein,

the stored data for specifying said first authentication device, which stores said history data as history data *K*, corresponds to secret data *C* and authentication data *R*, and the stored data for specifying said second authentication device, which stores said history data as history data *K*, corresponds to secret data *S* and authentication data *Q*.

3. The mutual authentication according to claim 2, wherein,

said first transmitting step newly generates the secret data *C* by use of the secret data *S* and the authentication data *R* of the history data K being stored, and newly generates the authentication data *R* of the history data K being stored, encrypts the generated new authentication data *R* by use of the

history data *K* to obtain authentication *A*, and transmits said authentication data *A* and the new secret data *C* to the second authentication device;

said first updating step receives data from said second authentication device, and updates the history data *K* by the new secret data *C* thus transmitted, the secret data *S* newly generated thus received, the authentication data *Q* newly generated thus received and said new authentication data *R* thus transmitted;

said second transmitting step receives data from said first authentication device, newly generates secret data *S* by use of the new secret data *C* thus received and the authentication data *Q* of the history data K being stored, and newly generates the authentication data *Q* of the history data K being stored, encrypts the generated new authentication data *Q* by use of the history data *K* being stored to obtain the authentication data B, transmits to the first authentication device said authentication data B and new secret data *S*; and

said second updating step updates said history data *K*, by the new secret data *C* thus received, the newly generated secret data *S*, the newly generated authentication data *Q*, and the new authentication data *R* thus received, wherein,

in at least one of said first authentication device and said second authentication device, when validity of the stored data is established based on the history data *K*, it is verified that the mutual relationship between the first authentication device and the second authentication device is valid.

4. The mutual authentication method according to claim 1, wherein,

said storing step stores as the history data, update results obtained by authentication in said first transmitting step, the first updating step, the second transmitting step and the second updating step.

5. The mutual authentication method according to claim 2, wherein,

at least one of the authentication data R and the authentication data Q is at least one of the followings: a random number generated by random number generating means, data volume, and time-related data.

6. The mutual authentication method according to claim 2, wherein,

in the first transmitting step of said first authentication device, a value of a computation result from a function predefined by said secret data S and said authentication data R is generated as the secret data C, and in the second transmitting step of said second authentication device, a value of a computation result from a function predefined by said secret data C and said authentication data Q is generated as the secret data S.

7. The mutual authentication method according to claim 2, wherein,

in the first transmitting step of said first authentication device, a value of a computation result from a

function predefined by said new authentication data *R* thus generated and said history data *K* is obtained as the authentication data *A*, and in the second transmitting step of said second authentication device, a value of a computation result from a function predefined by said new authentication data *Q* thus generated and said history data *K* is obtained as the authentication data B.

8. The mutual authentication method according to claim 2, wherein,

a verifying step of said first authentication device verifies that said mutual relationship is valid when a computation result of a predefined function by the stored authentication data *Q* out of said history data *K*, and the secret data *C* generated before previous transmission matches the secret data *S* thus received.

9. The mutual authentication method according to claim 2, wherein,

a verifying step of said second authentication device verifies that said mutual relationship is valid when a computation result of a predefined function by the stored secret data *S* and the authentication data *R* out of said history data *K* matches the secret data *C* thus received.

10. The mutual authentication method according to claim 2, wherein,

said storing step stores as the history data *K*, data obtained as a result of plural executions of said first

transmitting step, the second transmitting step, the first updating step and the second updating step.

11. A mutual authentication device comprising a first authentication device and a second authentication device being connected via a communication line, which authenticates a mutual relationship between said first authentication device and said second authentication device, including,

a first memory which is provided in said first authentication device and stores stored data for specifying the first authentication device,

a second memory which is provided in said second authentication device and stores stored data for specifying the second authentication device,

authentication data storing means which store the stored data by previous authentication per authentication carried out mutually in advance between said first authentication device and said second authentication device,

history data storing means which store as history data, an update result updated by use of said authentication data, commonly in each of said first authentication device and said second authentication device,

stored data generating means which are provided in an authentication device on a data-for-authentication transmitting side out of said first authentication device and said second authentication device, and generate new stored data by use of said history data,

first transmitting means which encrypt the thus generated

new stored data by use of said history data and transmit the encryption data to the authentication device on a data-for-authentication receiving side,

stored data generating means which are provided in the authentication device on the data-for-authentication receiving side, and generate new stored data by use of the stored data from the authentication device on said data-for-authentication transmitting side and the history data being stored,

second transmitting means which encrypt the new stored data thus generated by use of said history data, and return the encryption data to the authentication device on said data-for-authentication transmitting side,

first updating means which are provided in the authentication device on the data-for-authentication transmitting side and update said history data by the stored data returned from the authentication device on said data-for-authentication receiving side and the new stored data thus transmitted, and

second updating means which are provided in the authentication device on the data-for-authentication receiving side and update said history data by the stored data from the authentication device on said data-for-authentication transmitting side and said new stored data thus returned, and further comprising,

verifying means which verify that a mutual relationship between the first authentication device and the second authentication device is valid when validity of the stored data

is established based on said history data in at least one of said first authentication device and said second authentication device.

12. The mutual authentication device according to claim 11, further comprising,

computing means which compute data for authentication for encrypting the new stored data thus generated, by use of said history data.

13. The mutual authentication device according to claim 12, comprising,

random number generating means which generate data for encryption when the data for authentication is generated by said computing means.

14. A onetime ID generating method which generates identification information usable for just one time as onetime ID in authentication between a plurality of devices or applications, wherein,

in each of the devices or the applications which carry out said authentication, a variable shared key is generated which changes per predefined communication unit requiring said authentication, and a function value of one-way function is obtained, in which the variable shared key is used as an argument, and said onetime ID is generated based on the function value.

15. A onetime ID generating method which generates a

onetime ID assuming, as the onetime ID, the identification information usable just one time in authentication between a plurality of devices or applications, wherein,

in each of the devices or the applications which carry out said authentication, a variable shared key is generated which changes per predefined communication unit requiring said authentication, and simultaneously a function value of one-way function is obtained in which the variable shared key and information regarding a communication sequence or communication number of times are used as arguments, and said onetime ID is generated based on the function value.

16. A onetime ID generating method which generates a onetime ID assuming, as the onetime ID, identification information usable just one time in authentication between a plurality of devices or applications, wherein,

in each of the devices or the applications which carry out said authentication, a random number is generated within a predefined communication unit requiring said authentication, and simultaneously a function value of one-way function is obtained in which the random number and a predefined shared key are used as arguments, and said onetime ID is generated based on the function value.

17. A onetime ID generating method in which a onetime ID is generated in both one device and another device, assuming, as the onetime ID, identification information usable just one time in authentication between one device and the other device,

and simultaneously the one device transmits the onetime ID to the other device for the other device to compare and collate the onetime ID which the other device received from the one device with the onetime ID generated by the other device, so that the one device identifies or authenticates the other device, wherein,

the one device and the other device generate a variable shared key which changes per predefined communication unit requiring said authentication, and simultaneously, a function value of one-way function is obtained in which the variable shared key is used as an argument and the onetime ID is generated based on the function value.

18. A onetime ID generating method in which a onetime ID is generated in both one device and another device, assuming, as the onetime ID, identification information usable just one time in authentication between one device and the other device, and simultaneously the one device transmits the onetime ID to the other device for the other device to compare and collate the onetime ID which the other device received from the one device with the onetime ID generated by the other device, so that the one device identifies or authenticates the other device, wherein,

the one device and the other device generate a variable shared key which changes per predefined communication unit requiring said authentication, and simultaneously, a function value of one-way function is obtained in which the variable shared key and a communication sequence or a communication

number of times are used as arguments, and said onetime ID is generated based on the function value.

19. A onetime ID generating method in which a onetime ID is generated in both one device and another device, assuming, as the onetime ID, identification information usable just one time in authentication between one device and the other device, and simultaneously the one device transmits the onetime ID to the other device for the other device to compare and collate the onetime ID which the other device received from the one device with the onetime ID generated by the other device, so that the one device identifies or authenticates the other device, wherein,

the one device and the other device generate a random number within a predefined communication unit requiring said authentication, and simultaneously, a function value of one-way function is obtained in which the random number and a predefined shared key are used as arguments, and the onetime ID is generated based on the function value.

20. An authentication method which carries out authentication between devices and applications, assuming as onetime ID, identification information usable just one time, generates a variable shared key which changes per predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key is used as an argument, generates said

onetime ID from the function value, and carries out the authentication between a first device and a second device by use of the onetime ID thus generated, comprising:

a step in which said first device generates said onetime ID by use of the variable shared key, which is previously shared between said first and said second devices, and transmits to the second device the onetime ID thus generated, a function value of the one-way function Fc in which at least the ID predefined in the first device is used as an argument, and one of Diffie-Hellman public values previously stored in the first device;

a step in which said second device obtains by computation said onetime ID and a function value of said one-way function Fc, and determines validity of said first device by collating a computation result with the onetime ID received from said first device and the function value of the one-way function Fc;

a step in which said second device transmits to said first device, when said second device determines that said first device is valid, a function value of the one-way function Fs in which at least the ID predefined in the second device is used as an argument, and another of the Diffie-Hellman public values previously stored in the second device; and

a step in which said first device obtains by computation a function value of said one-way function Fs, and determines the validity of said second device by collating a result of the computation and the function value of the one-way function Fs received from said second device.

21. The authentication method according to claim 20, wherein,

as said one-way function Fc, a pseudo-random number function is used in which a predefined shared key, one of said above Diffie-Hellman public values, the ID predefined in said first device, and said above onetime ID are used as arguments, and simultaneously, as said one-way function Fs, a pseudo-random number function is used in which said predefined shared key, one of said Diffie-Hellman public values, the other of said Diffie-Hellman public values, the ID predefined in said second device, and said onetime ID are used as arguments.

22. An authentication method which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key which changes per predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key and information regarding a communication sequence or communication number of times are used as arguments, generates said onetime ID from the function value, and carries out the authentication between a first device and a second device by use of the onetime ID thus generated, comprising:

a step in which said first device generates, as a first onetime ID, a function value of one-way function in which a first variable shared key previously shared between said first device

and said second device, and information regarding the communication sequence of the first device are used as arguments, and simultaneously encrypts, by use of said first variable shared key, ID predefined in the first device, ID predefined in said second device, one of Diffie-Hellman public values previously stored in the first device and said first onetime ID, and transmits the thus encrypted data and said first onetime ID to said second device;

a step in which said second device obtains by computation said first onetime ID and identifies said first device by collating a result of the computation and said first onetime ID received from said first device;

a step in which said second device decodes said encryption data by use of said first variable shared key when said first device is identified, and determines validity of said first device based on the ID predefined in said first device, the ID predefined in said second device, and said first onetime ID, which are included in thus decoded data;

a step in which said second device generates, as a second onetime ID, a function value of one-way function in which said first variable shared key and information regarding a communication sequence of said second device are used as arguments when it is determined that said first device is valid, and simultaneously, generates as a second variable shared key, a Diffie-Hellman common key from one of the Diffie-Hellman public values received from said first device and the other of the Diffie-Hellman public values previously stored in the second device, and transmits to said first device, a function

value of one-way function *h* in which the second variable shared key, the ID predefined in said first device, the ID predefined in the second device and said second onetime ID are used as arguments, the other of Diffie-Hellman public values, and said second onetime ID;

a step in which the first device obtains by computation said second onetime ID, and the first device identifies said second device by collating a result of the computation and said second onetime ID received from said second device; and

a step in which said first device generates as said second variable shared key when the first device has identified said second device, a Diffie-Hellman common key from the other of said Diffie-Hellman public values received from said second device and the one of said Diffie-Hellman public values previously stored in the first device and simultaneously, obtains by computation a function value of said one-way function *h* by use of the second variable shared key, and determines validity of said second device by collating a result of the computation and the function value of the one-way function *h* received from said second device.

23. The authentication method according to claim 22, wherein,

as one-way function for generating said second onetime ID, a one-way function being different from the one-way function for generating said first onetime ID is used.

24. An authentication method which carries out

authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined variable shared key are used as arguments, generates a onetime ID from the function value, and carries out the authentication between a first device and a second device by use of the onetime ID thus generated, comprising:

a step in which said first device generates a first random number and simultaneously obtains as a first onetime ID, a function value of one-way function in which said first shared key previously shared between the first device and said second device is used as an argument, and transmits the first onetime ID and said first random number to said second device;

a step in which said second device generates a second random number and simultaneously obtains as a second onetime ID, a function value of one-way function in which said first random number and the first shared key are used as arguments, and transmits to said first device the second onetime ID and said second random number;

a step in which said first device obtains by computation said second onetime ID based on said first random number and said first shared key, and determines validity of said second device by comparing a result of the computation with said second onetime ID received from said second device;

a step in which said first device generates a second shared key based on said first random number and said second random number, and simultaneously obtains as a third onetime ID, a function value of one-way function in which the second shared key, said first random number and said second random number are used as arguments, and transmits the third onetime ID to said second device; and

a step in which said second device generates said second shared key based on said first random number and said second random number, and simultaneously, obtains by computation said third onetime ID based on the second shared key, said first random number and said second random number, and determines validity of said first device by comparing a result of the computation with said third onetime ID received from said first device.

25. An authentication method which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined variable shared key are used as arguments, generates a onetime ID from the function value, and carries out the authentication between a first device and a second device by use of the onetime ID thus generated, comprising:

a step in which said first device generates a first random number and simultaneously obtains as a first onetime ID, a function value of one-way function in which a shared key previously shared between the first device and said second device is used as an argument, and transmits to said second device the first onetime ID and said first random number;

a step in which said second device generates a second random number and simultaneously obtains as a second onetime ID, a function value of one-way function in which a first random number and said shared key are used as arguments, and transmits to said first device the second onetime ID and said second random number;

a step in which said first device obtains by computation said second onetime ID based on said first random number and said shared key, and determines validity of said second device by comparing a result of the computation and said second onetime ID received from said second device;

a step in which said first device generates, as the third onetime ID, a function value of one-way function in which said first random number, said second random number, and said shared key are used as arguments, and transmits the third onetime ID to said second device; and

a step in which said second device generates by computation said third onetime ID based on said first random number, said second random number and said shared key, and determines validity of said first device by comparing a result of the computation and said third onetime ID received from said first device.

26. The authentication method according to claim 24, wherein,

said first random number and said second random number are transmitted in a state as being encrypted by a shared key previously shared between said first device and said second device.

27. The authentication method according to claim, wherein,

said first random number and said second random number are transmitted in a state as being encrypted by a shared key previously shared between said first device and said second device.

28. The authentication method according to any one of claims 24 to 26, wherein,

in the step where said second device transmits to said first device said second onetime ID and said second random number, said second device has, as an initial random number, a random number shared between the second device and said first device, and carries out a predefined computation in which the initial random number and said first random number are used as arguments, and transmits a result of the computation to said first device, and said first device uses said result of the computation received from said second device as a material for determining validity of said second device, together with said second onetime ID.

29. The authentication method according to claim 24, wherein,

in the step where said first device transmits said third onetime ID to said second device, said first device carries out a predefined computation in which said first random number and said second random number are used as arguments, and transmits a result of the computation to said second device, and said second device uses said result of the computation received from said first device as a material for determining validity of said first device, together with said third onetime ID.

30. The authentication method according to claim 25, wherein,

in the step where said first device transmits said third onetime ID to said second device, said first device carries out a predefined computation in which said first random number and said second random number are used as arguments, and transmits a result of the computation to said second device, and said second device uses said result of the computation received from said first device as a material for determining validity of said first device, together with said third onetime ID.

31. An authentication method which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring authentication in each of the

devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined variable shared key are used as arguments, generates a onetime ID from the function value, and carries out the authentication between a first device and a second device by use of the onetime ID thus generated, comprising:

a step in which said first device generates a first random number, simultaneously obtains as a first onetime ID, a function value of one-way function in which a shared key previously shared between the first device and said second device, the first stored random number and the second stored random number are used as arguments, and transmits to said second device, first encryption data which is obtained by encrypting with said shared key, the ID predefined in the first device, the ID predefined in said second device, and the first random number, together with said first onetime ID;

a step in which said second device obtains by computation said first onetime ID, and said first device is identified by collating a result of the computation and said first onetime ID received from said first device;

a step in which said second device decodes said first encryption data by use of said shared key when said second device has identified said first device, and validity of said first device is determined, based on the ID predefined in said first device and the ID predefined in the second device, which are included in the thus decoded data;

a step in which said second device generates a second

random number when said first device is determined to be valid, and simultaneously obtains as a second onetime ID, a function value of one-way function in which said first random number, said second stored random number and said shared key are used as arguments, and transmits to said first device the second encryption data, which is obtained by encrypting with said shared key, the ID predefined in said first device, the ID predefined in said second device, and said second random number, together with said second onetime ID;

a step in which said second device replaces said first stored random number and said second stored random number, respectively, with said first random number and said second random number;

a step in which said first device obtains by computation said second onetime ID, and said second device is identified by collating a result of the computation and said second onetime ID received from said second device;

a step in which said first device decodes said second encryption data by use of said shared key when said first device has identified said second device, validity of said second device is determined based on the ID predefined in said second device and the ID predefined in said first device, which are included in the thus decoded data; and

a step in which said first device replaces said first stored random number and said second stored random number, respectively, with said first random number and said second random number.

32. The authentication method according to claim 31, wherein,

after said first stored random number and said second stored random number are respectively replaced with said first random number and said second random number, the shared key is varied by generating said shared key based on the first random number and the second random number.

33. A server which carries out authentication between devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key is used as an argument, generates said onetime ID from the function value, and carries out the authentication between the server and a client, by use of the onetime ID thus generated, comprising:

receiving means which receive from said client, a function value of the one-way function Fc in which at least a client ID predefined in said client is used as an argument, one of Diffie-Hellman public values previously stored in said client, and said onetime ID;

determining means which obtain by computation a function value Fc of said one-way function and said onetime ID, and determine validity of said client by comparing a result of the computation with said onetime ID received from said client and

the function value of said one-way function Fc; and

transmitting means which transmit to said client, when said determining means determine that said client is valid, a function value of one-way function Fs in which the server ID predefined in the server is used as an argument, and another of the Diffie-Hellman public values predefined in the server.

34. A client which carries out authentication between devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key is used as an argument, generates a onetime ID from the function value, and carries out the authentication between the server and the client, by use of the onetime ID thus generated, comprising:

transmitting means which generate said onetime ID by use of the variable shared key previously shared between the client and said server, and simultaneously obtain a function value of one-way function Fc in which at least a client ID predefined in the client is used as an argument, and transmit to said server the onetime ID, the function value of the one-way function Fc, and one of Diffie-Hellman public values previously stored in the client;

receiving means which receive from said server a function value of one-way function Fs in which at least the server ID

predefined in said server is used as an argument and another of Diffie-Hellman public values previously stored in said server; and

determining means which obtain by computation a function value of said one-way function Fs, and determine validity of said server by comparing a result of the computation with the function value of said one-way function Fs received from said server.

35. An authentication system comprising a server and a client, in which said server and said client carry out authentication between devices or applications, assuming, as onetime ID identification information usable just one time, generate a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtain a function value of a one-way function in which the variable shared key is used as an argument, generates said onetime ID from the function value, and carries out the authentication between the server and a client, by use of the onetime ID thus generated,

said server comprising:

receiving means which receive from said client, a function value of the one-way function Fc in which at least a client ID predefined in said client is used as an argument, one of Diffie-Hellman public values previously stored in said client, and said onetime ID;

determining means which obtain by computation a function

value Fc of said one-way function and said onetime ID, and determine validity of said client by comparing a result of the computation with said onetime ID received from said client and the function value of said one-way function Fc; and

transmitting means which transmits to said client, when said determining means determine that said client is valid, a function value of one-way function Fs in which the server ID predefined in the server is used as an argument, and another of the Diffie-Hellman public values predefined in the server, and

said client comprising:

transmitting means which generate said onetime ID by use of the variable shared key previously shared between said client and said server, and simultaneously obtain a function value of one-way function Fc in which at least the client ID predefined in the client is used as an argument, and transmit to said server the onetime ID, the function value of the one-way function Fc, and the one of Diffie-Hellman public values previously stored in the client;

receiving means which receive from said server a function value of the one-way function Fs in which at least the server ID predefined in the server is used as an argument and the other of Diffie-Hellman public values previously stored in said server; and

determining means which obtain by computation, a function value of said one-way function Fs, and determine validity of said server by comparing a result of the computation with the function value of said one-way function Fs received from said

server.

36. A program to be executed by a server which carries out authentication between devices or applications, assuming as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key is used as an argument, generates a onetime ID from the function value, and carries out the authentication with a client by use of the onetime ID thus generated, comprising:

a process which receives from a client a function value of one-way function Fc in which at least a client ID predefined in said client is used as an argument, one of Diffie-Hellman public values previously stored in said client, and said onetime ID;

a process which obtains by computation a function value of said one-way function Fc and said onetime ID, and determines validity of said client by comparing a result of the computation with said onetime ID received from said client and the function value of said one-way function Fc; and

a process which transmits to said client, when said client is determined to be valid, a function value of the one-time function Fs in which at least the server ID predefined in said server is used as an argument and another of the Diffie-Hellman public values previously stored in said server.

37. A program to be executed by a client which carries out authentication between devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key is used as an argument, generates a onetime ID from the function value, and carries out the authentication with a server by use of the onetime ID thus generated, comprising:

a process which generates said onetime ID by use of the variable shared key previously shared between the client and said server, obtains by computation a function value of one-way function Fc in which at least a client ID predefined in said client is used as an argument, and transmits to said server the onetime ID, the function value of the one-way function Fc, and one of Diffie-Hellman public values previously stored in said client;

a process which receives a function value of one-way function Fs in which at least the server ID predefined in said server is used as an argument and the other of the Diffie-Hellman public values previously stored in said server; and

a process which obtains by computation a function value of said one-way function Fs, and determines validity of said server, by comparing a result of the computation with the function value of said one-way function Fs received from said

server.

38. A server which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key and information regarding communication sequence or communication number of times are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a client, by use of the onetime ID thus generated, comprising:

receiving means which assume, as a first onetime ID, a function value of one-way function in which the first variable shared key previously shared between the client and said server and the information regarding the communication sequence of said client are used as arguments, and receive from said client encryption data which is obtained by encrypting with said first variable shared key, the first onetime ID, the client ID predefined in said client, the server ID predefined in the server, and one of Diffie-Hellman public values previously stored in said client, together with said first onetime ID;

determining means which obtain by computation said first onetime ID, identifies said client by collating a result of the computation with said onetime ID received from said client, decodes said encryption data by use of said first variable

shared key when said client has been identified, and determine validity of said client based on said client ID, said server ID and said first onetime ID, which are included in the thus decoded data; and

transmitting means which generate as a second onetime ID, a function value of one-way function in which said first variable shared key and information regarding a communication sequence of the server are used as arguments, and simultaneously, generate as a second variable shared key, a Diffie-Hellman common key from the one of the Diffie-Hellman public values received from said client and another of the Diffie-Hellman public values previously stored in the server, and transmit to said client a function value of one-way function *h* in which the second variable shared key, said client ID, said server ID and said second onetime ID are used as arguments, said other of Diffie-Hellman public values, and said second onetime ID.

39. A client which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the variable shared key and information regarding a communication sequence or communication number of times are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a client, by use of the onetime ID

thus generated, comprising:

transmitting means which generate as a first onetime ID, a function value of one-way function in which the first variable shared key previously shared between the client and said server and information regarding a communication sequence of the client are used as arguments, and simultaneously by use of said first variable shared key, encrypt the client ID predefined in the client, the server ID predefined in said server, and one of Diffie-Hellman public values previously stored in the client, and said first onetime ID, and transmit to said server thus encrypted data and said first onetime ID;

receiving means which assume, as the second onetime ID, a function value of the one-way function in which said first variable shared key and the information regarding the communication sequence of said server are used as arguments, assume a Diffie-Hellman common key as the second variable shared key, and receive a function value of the one-way function *h* in which said second onetime ID, said second variable shared key, said client ID and said server ID are used as arguments, the other of the Diffie-Hellman public values previously stored in said server, and said second onetime ID; and

determining means which obtain by computation said second onetime ID, identifies said server by collating a result of the computation with said second onetime ID received from said server, when said server has been identified, generate a Diffie-Hellman common key, as said second variable shared key, from the other of said Diffie-Hellman public values received from said server and the one of said Diffie-Hellman public

values previously stored in the client, and simultaneously, obtain by computation a function value of the one-way function *h* by use of the second variable shared key, and determine validity of said server by collating a result of the computation and a function value of the one-way function *h* received from said server.

40. An authentication system comprising a server and a client, in which said server and said client carry out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generate a variable shared key changing per a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtain a function value of a one-way function in which the variable shared key and information regarding a communication sequence or communication number of times are used as arguments, generates a onetime ID from the function value, and carries out the authentication between the server and a client, by use of the onetime ID thus generated,

said server comprising:

receiving means which assume, as a first onetime ID, a function value of one-way function in which the first variable shared key previously shared between said client and said server and the information regarding the communication sequence of the client are used as arguments, and receive from said client encryption data which is obtained by encrypting with said first variable shared key, the first onetime ID, the client ID

predefined in said client, the server ID predefined in the server, and one of Diffie-Hellman public values previously stored in said client, together with said first onetime ID;

determining means which obtain by computation said first onetime ID, identifies said client by collating a result of the computation with said onetime ID received from said client, decode said encryption data by use of said first variable shared key when said client has been identified, and determine validity of said client based on said client ID, said server ID and said first onetime ID, which are included in the thus decoded data; and

transmitting means which generate as a second onetime ID, a function value of one-way function in which said first variable shared key and information regarding the communication sequence of the server are used as arguments, and simultaneously, generate as a second variable shared key, a Diffie-Hellman common key from the one of the Diffie-Hellman public values received from said client and another of the Diffie-Hellman public values previously stored in the server, and transmit to said client a function value of one-way function *h* in which the second variable shared key, said client ID, said server ID and said second onetime ID are used as arguments, the other of said Diffie-Hellman public values, and said second onetime ID, and

said client comprising:

transmitting means which generate as a first onetime ID, a function value of one-way function in which the first variable shared key previously shared between said client and said server and information regarding the communication sequence of the

client are used as arguments, and simultaneously by use of said first variable shared key, encrypt the client ID predefined in the client, the server ID predefined in said server, and the one of the Diffie-Hellman public values previously stored in the client, and said first onetime ID, and transmit to said server thus encrypted data and said first onetime ID;

receiving means which assumes, as the second onetime ID, a function value of the one-way function in which said first variable shared key and the information regarding the communication sequence of said server are used as arguments, assume the Diffie-Hellman common key as the second variable shared key, and receive a function value of the one-way function *h* in which said second onetime ID, said second variable shared key, said client ID and said server ID are used as arguments, the other of the Diffie-Hellman public values previously stored in said server, and said second onetime ID; and

determining means which obtain by computation said second onetime ID, identifies said server by collating a result of the computation with said second onetime ID received from said server, when said server has been identified, generate the Diffie-Hellman common key, as said second variable shared key, from the other of said Diffie-Hellman public values received from said server and the one of said Diffie-Hellman public values previously stored in the client, and simultaneously, obtain by computation a function value of said one-way function *h* by use of the second variable shared key, and determine validity of said server by collating a result of the computation and a function value of the one-way function *h* received from

said server.

41. A server which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a client, by use of the onetime ID thus generated, comprising:

first receiving means which assume, as a first onetime ID, a function value of the one-way function in which the first shared key previously shared between the server and said client is used as an argument, and receive from said client the first onetime ID and the first random number generated in said client;

transmitting means which generate a second random number and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number and said first shared key are used as arguments, and transmit to said client said second onetime ID and said second random number;

second receiving means which assume, as a third onetime ID, a function value of one-way function in which said first random number, said second random number and the second shared key are used as arguments, and receive the third onetime ID from said client; and

determining means which generate said second shared key based on said first random number and said second random number, and simultaneously, obtain by computation said third onetime ID based on said second shared key, said first random number and said second random number, and determine validity of said client by comparing a result of the computation with said third onetime ID received from said client.

42. A client which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a server, by use of the onetime ID thus generated, comprising:

first transmitting means which generate a first random number, and simultaneously obtain as a first onetime ID a function value of one-function in which a first shared key previously shared between the client and said server is used as an argument, transmit to said server the first onetime ID and said first random number;

receiving means which assume, as the second onetime ID, a function value of one-way function in which said first random number and said first shared key are used as augments, and receive from said server the second onetime ID and the second

random number generated in said server;

determining means which obtain by computation said second onetime ID based on said first random number and said first shared key, and determine validity of said server by comparing a result of the computation with said second onetime ID received from said server; and

second transmitting means which generate a second shared key based on said first random number and said second random number when it is determined that said server is valid by said determining means, and simultaneously obtain as a third onetime ID, a function value of one-way function in which the second shared key, said first random number and said second random number are used as arguments, and transmit to said server the third onetime ID.

43. An authentication system comprising a server and a client, in which said server and said client carry out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generate a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtain a function value of a one-way function in which the random number and the predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication mutually between the server and a client, by use of the onetime ID thus generated,

said server comprising:

first receiving means which assume, as a first onetime ID, a function value of the one-way function in which the first shared key previously shared between said server and said client is used as an argument, and receive from said client the first onetime ID and a first random number generated in said client;

transmitting means which generate a second random number and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number and said first shared key are used as arguments, and transmit to said client the second onetime ID and said second random number;

second receiving means which assume, as a third onetime ID, a function value of one-way function in which said first random number, said second random number and the second shared key are used as arguments, and receive the third onetime ID from said client; and

determining means which generate said second shared key based on said first random number and said second random number, and simultaneously, obtain by computation said third onetime ID based on said second shared key, said first random number and said second random number, and determine validity of said client by comparing a result of the computation with said third onetime ID received from said client, and

said client comprising:

first transmitting means which generate the first random number, and simultaneously obtain as the first onetime ID a function value of one-function in which the first shared key previously shared between the client and said server is used as an argument, transmit to said server the first onetime ID

and said first random number;

receiving means which assume, as the second onetime ID, a function value of one-way function in which said first random number and said first shared key are used as augments, and receive from said server the second onetime ID and the second random number generated in said server;

determining means which obtain by computation said second onetime ID based on said first random number and said first shared key, and determine validity of said server by comparing a result of the computation and said second onetime ID received from said server; and

second transmitting means which generate the second shared key based on said first random number and said second random number when it is determined that said server is valid by said determining means, and simultaneously obtain as a third onetime ID, a function value of one-way function in which the second shared key, said first random number and said second random number are used as arguments, and transmit to said server the third onetime ID.

44. A server which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from

the function value, and carries out the authentication with a client, by use of the onetime ID thus generated, comprising:

first receiving means which assume, as the first onetime ID, a function value of one-way function in which a shared key previously shared between the server and said client is used as an argument, and receive from said client the first onetime ID and the first random number generated in said client;

transmitting means which generate a second random number, and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number and said shared key are used as arguments, and transmit to said client the second onetime ID and said second random number;

second receiving means which assume, as a third onetime ID, a function value of one-way function in which said shared key, said first random number and said second random number are used as arguments, and receive from said client the third onetime ID; and

determining means which obtain by computation said third onetime ID based on said first random number, said second random number and said shared key, and determine validity of said client by comparing a result of the computation and said third onetime ID received from said client.

45. A client which carries out authentication between plural devices or applications, assuming, as onetime ID identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications

carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a server, by use of the onetime ID thus generated, comprising:

first transmitting means which generate a first random number, obtain as a first onetime ID, a function value of one-way function in which a shared key previously shared between the client and said server is used as an argument, and transmit to said server the first onetime ID and said first random number;

receiving means which assume, as a second onetime ID, a function value of one-way function in which said first random number and said shared key are used as arguments, and receive from said server the second onetime ID and the second random number generated in said server;

determining means which obtain by computation said second onetime ID based on said first random number and said shared key, and determine validity of said server by comparing a result of the computation with said second onetime ID received from said server; and

second transmitting means which obtain as a third onetime ID, a function value of the one-way function in which said first random number, said second random number and said shared key are used as arguments when said server is determined to be valid by said determination means, and transmit to said server the third onetime ID.

46. An authentication system comprising a server and a

client, in which the server and the client carry out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generate a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtain a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication mutually between the server and a client, by use of the onetime ID thus generated,

said server comprising:

first receiving means which assume, as a first onetime ID, a function value of one-way function in which a shared key previously shared between said server and said client is used as an argument, and receive from said client the first onetime ID and a first random number generated in said client;

transmitting means which generate a second random number, and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number and said shared key are used as arguments, and transmit to said client the second onetime ID and said second random number;

second receiving means which assume as a third onetime ID, a function value of one-way function in which said shared key, said first random number and said second random number are used as arguments, and receive from said client the third onetime ID; and

determining means which obtain by computation said third

onetime ID based on said first random number, said second random number and said shared key, and determine validity of said client by comparing a result of the computation and said third onetime ID received from said client, and

said client comprising:

first transmitting means which generate the first random number, obtain as the first onetime ID, a function value of one-way function in which a shared key previously shared between said client and said server is used as an argument, and transmit to said server the first onetime ID and said first random number;

receiving means which assumes, as a second onetime ID, a function value of one-way function in which said first random number and said shared key are used as arguments, and receive from said server the second onetime ID and the second random number generated in said server;

determining means which obtain by computation said second onetime ID based on said first random number and said shared key, and determine validity of said server by comparing a result of the computation with said second onetime ID received from said server; and

second transmitting means which obtain as the third onetime ID, a function value of the one-way function in which said first random number, said second random number and said shared key are used as arguments when said server is determined to be valid by said determination means, and transmit to said server the third onetime ID.

47. A server which carries out authentication between

plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a client, by use of the onetime ID thus generated, comprising:

receiving means which assume, as a first onetime ID, a function value of one-way function in which the shared key previously shared between the server and said client, the first stored random number and the second stored random number are used as arguments, receive the first onetime ID from said client and simultaneously receive from said client, first encryption data which is obtained by encrypting with said shared key, the first random number generated in said client, a client ID predefined in said client and a server ID predefined in the server;

determining means which obtain by computation said first onetime ID, identify said client by collating a result of the computation with said first onetime ID received from said client, decode the first encryption data by use of said shared key when said client has been identified, and determine validity of said client based on said client ID and said server ID included in thus decoded data;

transmitting means which generate a second random number when said determining means determine that said client is valid,

and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number, said second stored random number and said shared key are used as arguments, and transmit to said client second encryption data which is obtained by encrypting with said shared key said client ID, said server ID and said second random number, together with said second onetime ID; and

replacing means which replace said first stored random number and said second stored random number respectively with said first random number and said second random number.

48. A client which carries out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generates a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication, obtains a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication with a server, by use of the onetime ID thus generated, comprising:

transmitting means which generate a first random number, obtain as a first onetime ID, a function value of one-way function in which a shared key previously shared between the client and said server, the first stored random number, and the second stored random number are used as arguments, and transmit to said server, first encryption data which is obtained by encrypting with said shared key, a client ID predefined in the

client, a server ID predefined in said server and said first random number, together with said first onetime ID;

receiving means which assume, as a second onetime ID, a function value of one-way function in which said first random number, said second stored random number and said shared key are used as arguments, receive said second onetime ID from said server, and simultaneously receive from said server second encryption data which is obtained by encrypting with said shared key the second random number generated in said server, said client ID and said server ID;

determining means which obtain by computation said second onetime ID, identify said server by collocating a result of the computation with said second onetime ID received from said server, decode said second encryption data by use of said shared key when said server has been identified, and determine validity of said server based on said server ID and said client ID included in thus decoded data; and

replacing means which replace said first stored random number and said second stored random number respectively with said first random number and said second random number.

49. An authentication system comprising a server and a client, in which said server and said client carry out authentication between plural devices or applications, assuming, as onetime ID, identification information usable just one time, generate a random number within a predefined communication unit requiring said authentication in each of the devices and applications carrying out said authentication,

obtain a function value of a one-way function in which the random number and a predefined shared key are used as arguments, generates said onetime ID from the function value, and carries out the authentication mutually between the server and a client, by use of the onetime ID thus generated,

said server comprising:

receiving means which assume, as a first onetime ID, a function value of one-way function in which the shared key previously shared between the server and client, a first stored random number and a second stored random number are used as arguments, receive the first onetime ID from said client and simultaneously receive from said client, first encryption data which is obtained by encrypting with said shared key, the first random number generated in said client, a client ID predefined in said client and a server ID predefined in the server;

determining means which obtain by computation said first onetime ID, identify said client by collating a result of the computation with said first onetime ID received from said client, decode said first encryption data by use of said shared key when said client has been identified, and determine validity of said client based on said client ID and said server ID included in thus decoded data;

transmitting means which generate a second random number when said determining means determine that said client is valid, and simultaneously obtain as a second onetime ID, a function value of one-way function in which said first random number, said second stored random number and said shared key are used as arguments, and transmit to said client second encryption data

which is obtained by encrypting with said shared key said client ID, said server ID and said second random number, together with said second onetime ID; and

replacing means which replace said first stored random number and said second stored random number respectively with said first random number and said second random number, and

said client comprising:

transmitting means which generate the first random number, obtain as the first onetime ID, a function value of one-way function in which a shared key previously shared between said client and said server, the first stored random number, and the second stored random number are used as arguments, and transmit to said server, first encryption data which is obtained by encrypting with said shared key, the client ID predefined in the client, the server ID predefined in said server and said first random number, together with said first onetime ID;

receiving means which assume, as the second onetime ID, a function value of one-way function in which said first random number, said second stored random number and said shared key are used as arguments, receive the second onetime ID from said server, and simultaneously receive from said server, second encryption data which is obtained by encrypting with said shared key the second random number generated in said server, said client ID and said server ID;

determining means which obtain by computation said second onetime ID, identify said server by collocating a result of the computation with said second onetime ID received from said server, decode said second encryption data by use of said shared

key when said server has been identified, and determine validity of said server based on said server ID and said client ID included in thus decoded data; and

replacing means which replace said first stored random number and said second stored random number respectively with said first random number and said second random number.

50. The authentication system according to claim 49, wherein,

after said server and said client replace said first stored random number and said second stored random number respectively with said first random number and said second random number, variation of the shared key is made by generating said shared key based on the first stored random number and the second stored random number.